Data Protection Starts With Data Classification

Devin Cambridge,
Global Managing Director

2014

First Data™

Beyond the transaction℠

Classifications for Government

First Data™

Beyond the transaction℠

Where would I look for information?

- Federal Information Processing Standard – FIPS199 (Classification)
  - The National Institute of Standards and Technology Issues the FIPS guidelines and definitions.
  - The FedRAMP FIPS 199 Categorization (Template)c an be used as a template to classify your information

- NIST 800 (FIPS 200) – General Information Security Framework to be compliant with FISMA items.

First Data™

Beyond the transaction℠

What is the FIPS-199 Data Classification Tag

- CIA= Confidentiality, Integrity, Availability
  - Is the stated goals under security theory.
    - **Confidentiality: Appropriate Visibility**
    - **Integrity: Correctness**
    - **Availability: Readily Accessible**
- **SC** information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},
- Where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.

SC = Security Classification

First Data.

Beyond the transaction.

Other Common Classifications

Public, Internal ,Confidential; Restricted	
Public	Published externally normally for marketing purposes or product support.
Internal	General Company Broadcasts and internal operation communications
Confidential	Executive Communications, Business Operations, Strategic Information, Intellectual Property
Restricted	Regulated Information , Financially Impacting, Core Datasets, Customer Data

First Data.

Beyond the transaction.

Other Common Classifications

Restricted (Paramilitary)- EC, Compartmentalized	
EC – Export Controlled:	Dual Use, Sanctioned information (ex. DOC Bureau of Industry and Security; DOS Directorate of Trade Controls)
Compartmentalized:	Special Clearance above restricted

First Data™

Beyond the transaction℠

Controls

First Data™

Beyond the transaction℠

Classification Controls

The linchpins of security

Once a classification system has been defined, tagging and enforcement is necessary

Things to consider:

How will you find items to tag?

- Sensitive Data Discovery Program (often a feature of your Data Loss Prevention technology [DLP])

How will you automate the tagging?

- Look again for your DLP vendor or Security Vendor

How will you prevent leakage of data (exfiltration)

- Again, look to DLP

How will you contain sensitive data? Did you create a space separate from your general network for sensitive data? Are you watching your endpoints for exfiltration of your data?

- Create special servers with extended controls
  - Encryption at Rest
  - Encryption in Motion
  - Privileged User Protection (Cryptographic Key Control)

First Data™

Beyond the transaction℠

Classification & Identity

The linchpins of security

For sensitive data repositories, use two(+) factor authentication for identity:

1. Password (Active Directory [AD])
2. Certificate (preferably not from the same AD forest; good for machine authentication)
3. One time password generation (RSA ACE one time password server)
4. Kerberos
5. Challenge Response System

Try not to use combine too many user interactive methods.

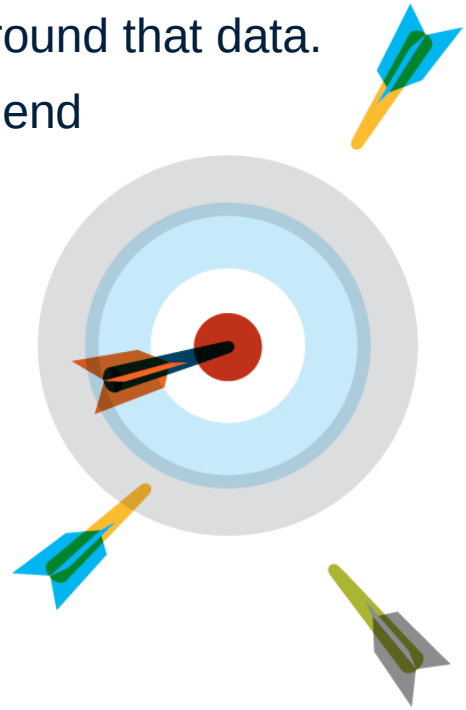
First Data™

Beyond the transaction℠

Reduce the Target

If it's not there it can't be used against you

- Reduce your infrastructure
- Reduce your entrance points to sensitive data repositories
- Guard the essential data and protect/monitor workers around that data.
- Force connections in and out through a ETL or if end to end encryption, through a specific route/gateway



First Data™

Beyond the transaction℠

Advanced Data Classification Techniques.

Cloud and Mobile

- Cloud
  - Keep your key management and authentication in house
    - Be careful of federated identity
  - Encryption is critical (Look at High Security Modules)
  - Use Data Loss Prevention tools to prevent sensitive information before going out via encryption
  - Killswitch your cloud servers if possible
- Mobile
  - Container Technologies (Encrypted containers Good Technologies)
  - Endpoint Protection w DLP & Program Execution Blocking (Verdasys)
  - Network to Mobile protection & E-mail Data Loss Prevention (Proofpoint, Symantec)

First Data.

Beyond the transaction.

Thank you.